AMENDMENTS TO THE CLAIMS

1. (Previously Presented) A policy-based network security management system, the system comprising:

a security management controller comprising one or more processors;

a computer-readable medium carrying one or more sequences of instructions for policy-based network security management, wherein execution of the one or more sequences of instructions by the one or more processors causes the one or more processors to perform the steps of:

receiving a set of data regarding a user of a network, wherein the set of data is a first set of data that is collected over a first duration of time;

receiving a second set of data that is collected over a second duration of time, wherein the first duration of time is shorter than the second duration of time;

creating and storing a risk level of the user based on the second set of data, wherein the second duration of time is sufficient to collect historical data regarding past malicious activities of the user, and wherein the risk level is a discrete value representing a long-term measurement of the likelihood of the user harming the network;

creating and storing a current alert level based on the first set of data, wherein the first duration of time is of a length appropriate for assessing current activities of the user, and wherein the current alert level is a discrete value representing a current measurement of the likelihood of the user negatively affecting the network;

automatically deciding on a course of action based on the risk level and the current alert level, wherein the course of action may be adverse to the user although the current alert level is insufficient to establish whether the user is performing a malicious action; and

sending signals to one or more network elements in the network to implement the course of action.

2. (Original) The system of Claim 1, wherein the set of data includes at least one or more alerts related to the user.

3. (Original) The system of Claim 1, wherein the signals include multiple alerts generated by multiple users; and the system further comprising sequences of instructions for correlating the multiple alerts to the multiple users.

4-5. (Canceled)

6. (Previously Presented) The system of Claim 1, further comprising sequences of instructions for performing the steps of:
receiving signals related to an external source including at least an alert assessment relevant to the network as a whole; and
creating and storing a current alert level value based on the alert assessment.

7. (Original) The system of Claim 1, further comprising sequences of instructions for performing the steps of:
receiving signals carrying performance information related to a health level of the network; and
determining the course of action based at least in part on the set of data and the performance information.

8. (Original) The system of Claim 1 further comprising:
a plurality of routers for routing information sent by users and servers to a variety of destinations;
a subscriber management system for managing a network;
a controller for executing the sequences of instructions;
a network element for generating input for the set of data; and
sequences of instructions for sending signals to the network elements.

9-15. (Canceled)

16. (Previously Presented) A method of providing policy-based network security management, comprising the steps of:

receiving a set of data regarding a user of a network, wherein the set of data is a first set of data that is collected over a first duration of time;

receiving a second set of data that is collected over a second duration of time, wherein the first duration of time is shorter than the second duration of time;

creating and storing a risk level of the user based on the second set of data, wherein the second duration of time is sufficient to collect historical data regarding past malicious activities of the user, and wherein the risk level is a discrete value representing a long-term measurement of the likelihood of the user harming the network;

creating and storing a current alert level based on the first set of data, wherein the first duration of time is of a length appropriate for assessing current activities of the user, and wherein the current alert level is a discrete value representing a current measurement of the likelihood of the user negatively affecting the network;

automatically deciding on a course of action based on the risk level and the current alert level, wherein the course of action may be adverse to the user although the current alert level is insufficient to establish whether the user is performing a malicious action; and

sending signals to one or more network elements in the network to implement the course of action.

17. (Original) The method of Claim 16 wherein the set of data includes at least one or more alerts related to the user.

18. (Original) The method of Claim 16, wherein the signals include multiple alerts generated by multiple users, and the method further comprises correlating the multiple alerts to the multiple users.

19-20. (Canceled)

21. (Previously Presented) The method of Claim 16 further comprising receiving signals related to an external source including an alert assessment relevant to the network as a whole, wherein the current alert level is also based on the alert assessment.

22. (Original) The method of Claim 16 further comprising receiving signals carrying performance information related to a health level of the network, wherein the course of action is based on the set of data and the performance information.

23-26. (Canceled)

27. (Previously Presented) A method of policy-based network security management, comprising the computer-implemented steps of:

collecting network performance statistics related to an overall health of a network and individual performance statistics of one or more individual units of the network, the collecting being performed by a performance management system;

sending the network performance statistics to a controller for analysis;

computing an overall health state based on the network performance statistics and the individual performance statistics, using the controller;

reading external alert data from an external alert source, using the controller;

collecting security event data from the network;

sending the security event data to a fault management system;

using the fault management system for checking for duplications in the security event data, and deduplicating duplicate security events in the security event data;

calculating an alert state based on the security event data from the fault management system and the external alert data, wherein the alert state is a

discrete value representing a current measurement of the likelihood of the network being negatively affected;

obtaining user information from a subscriber management system;

correlating the security event data from the fault management system with the user information to form correlated security event data;

reading external user risk data from an external user risk source into the controller;

calculating a user risk state based on the correlated security event data and the external user risk data, using the controller, wherein the user risk state is a discrete value representing a long-term measurement of the likelihood of the network being harmed;

calculating a decision regarding whether to take corrective action based on the overall health state, the alert state, and the user risk state, using the controller;

sending the decision from the controller to the subscriber management system; and

sending directives, related to the decision, from the subscriber management system to the network.

28. (Previously Presented) A system comprising:

a fault management system that receives network security data and deduplicates duplicate indications of security events in the network security data to form deduplicated security event data;

a subscriber management system that manages subscribers using a network, wherein the subscriber management system stores subscriber information about individual users and is capable of sending directives to the individual users based on a decision to take corrective action toward the individual users;

wherein the deduplicated security event data from the fault management system is correlated to the subscriber information to form correlated network security data;

a performance management system that receives overall performance data related to an overall health of the network and individual performance data related to a health of one or more individual units of the network; and

a controller that:

receives external alert data from an external alert source, external user risk data from an external user risk source, the deduplicated security event data, the correlated network security data, the overall performance data, and the individual performance data;

computes an alert state based on at least the external alert data and the deduplicated security event data, wherein the alert state is a discrete value representing a current measurement of the likelihood of the network being negatively affected;

computes a user risk state based on at least the external user risk data and the correlated network security data, wherein the user risk state is a discrete value representing a long-term measurement of the likelihood of the network being harmed;

computes a health state based on at least the overall performance data and the individual performance data;

makes the decision whether to take corrective action based on at least the alert state, the user risk state, and the health state; and

causes directives that implement the decision to be sent to the network.

29. (Previously Presented) An apparatus for providing policy-based network security management, comprising:

means for receiving a set of data regarding a user of a network, wherein the set of data is a first set of data that is collected over a first duration of time;

means for receiving a second set of data that is collected over a second duration of time, wherein the first duration of time is shorter than the second duration of time;

means for creating and storing a risk level of the user based on the second set of data, wherein the second duration of time is sufficient to collect historical data

regarding past malicious activities of the user, and wherein the risk level is a discrete value representing a long-term measurement of the likelihood of the user harming the network;

means for creating and storing a current alert level based on the first set of data, wherein the first duration of time is of a length appropriate for assessing current activities of the user, and wherein the current alert level is a discrete value representing a current measurement of the likelihood of the user negatively affecting the network;

means for automatically deciding on a course of action based on the risk level and the current alert level, wherein the course of action may be adverse to the user although the current alert level is insufficient to establish whether the user is performing a malicious action; and

means for sending signals to one or more network elements in the network to implement the course of action.

30. (Canceled)

31. (New) The apparatus of Claim 29, wherein the first set of data includes at least one or more alerts related to the user.

32. (New) The apparatus of Claim 29, wherein the signals include multiple alerts generated by multiple users; and the apparatus further comprises means for correlating the multiple alerts to the multiple users.

33. (New) The apparatus of Claim 29, further comprising:

means for receiving signals related to an external source including at least an alert assessment relevant to the network as a whole; and

means for creating and storing a current alert level value based on the alert assessment.

34. (New) The apparatus of Claim 29, further comprising:
means for receiving signals carrying performance information related to a health level of the network; and
means for determining the course of action based at least in part on the set of data and the performance information.

35. (New) The apparatus of Claim 29, further comprising:
means for communicatively connecting to a plurality of routers that route information sent by users and servers to a variety of destinations;
means for communicatively connecting to a subscriber management system for managing a network;
means for communicatively connecting to a network element for generating input for the first set of data; and
means for sending signals to the network element.